vTCP for ALG Support

Virtual Transport Control Protocol (vTCP) functionality provides a framework for various Application Layer Gateway (ALG) protocols to appropriately handle the Transport Control Protocol (TCP) segmentation and parse the segments in the Cisco firewall, Network Address Translation (NAT) and other applications.

Prerequisites for vTCP for ALG Support

Your system must be running Cisco IOS XE Release 3.1 or a later Cisco IOS XE software release. The latest version of NAT or firewall ALG should be configured.

Restrictions for vTCP for ALG Support

- To aid ALG payload parsing, vTCP supports reassembly of TCP segments. In order to protect system resources, the amount of memory that vTCP can consume for reassembly is restricted to 8K for FTP, H323, LDAP, NETBIOS, PPTP, SCCP, SUNRPC, and TFTP. Connections will be reset once the limits are reached.
- vTCP does not support the high availability functionality. High availability mainly relies on the firewall or Network Address Translation (NAT) to synchronize the session information to the standby forwarding engine.
- vTCP does not support asymmetric routing. vTCP validates and assembles packet segments based on their sequence number. If packet segments that belong to the same Layer 7 message go through different devices, vTCP will not record the proper state or do an assembly of these segments.

Information About vTCP for ALG Support

Overview of vTCP for ALG Support

When a Layer 7 protocol uses TCP for transportation, the TCP payload can be segmented due to various reasons, such as application design, maximum segment size (MSS), TCP window size, and so on. The application-level gateways (ALGs) that the firewall and NAT support do not have the capability to recognize TCP fragments for packet inspection. vTCP is a general framework that ALGs use to understand TCP segments and to parse the TCP payload.

vTCP helps applications like NAT and Session Initiation Protocol (SIP) that require the entire TCP payload to rewrite the embedded data. The firewall uses vTCP to help ALGs support data splitting between packets.

When you configure firewall or NAT ALGs, the vTCP functionality is activated.

vTCP currently supports Real Time Streaming Protocol (RTSP) and DNS ALGs.

TCP Acknowledgment and Reliable Transmission

Because vTCP resides between two TCP hosts, a buffer space is required to store TCP segments temporarily, before they are sent to other hosts. vTCP ensures that data transmission occurs properly between hosts. vTCP sends a TCP acknowledgment (ACK) to the sending host if vTCP requires more data for data transmission. vTCP also keeps track of the ACKs sent by the receiving host from the beginning of the TCP flow to closely monitor the acknowledged data.

vTCP reassembles TCP segments. The IP header and the TCP header information of the incoming segments are saved in the vTCP buffer for reliable transmission.

vTCP can make minor changes in the length of outgoing segments for NAT-enabled applications. vTCP can either squeeze the additional length of data to the last segment or create a new segment to carry the extra data. The IP header or the TCP header content of the newly created segment is derived from the original incoming segment. The total length of the IP header and the TCP header sequence numbers are adjusted accordingly.

vTCP with NAT and Firewall ALGs

ALG is a subcomponent of NAT and the firewall. Both NAT and the firewall have a framework to dynamically couple their ALGs. When the firewall performs a Layer 7 inspection or NAT performs a Layer 7 fix-up, the parser function registered by the ALGs is called and ALGs take over the packet inspection. vTCP mediates between NAT and the firewall and the ALGs that use these applications. In other words, packets are first processed by vTCP and then passed on to ALGs. vTCP reassembles the TCP segments in both directions within a TCP connection.

How to Configure vTCP for ALG Support

The RTSP, DNS, NAT, and the firewall configurations enable vTCP functionality by default. Therefore no new configuration is required to enable vTCP functionality.

Enabling RTSP to Activate vTCP

Perform this task to enable RTSP packet inspection.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **class class-default**
10. **exit**
11. **exit**
12. **zone security** *zone-name1*
13. **exit**
14. **zone security** *zone-name2*
15. **exit**
16. **zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name*
17. **service-policy type inspect** *policy-map-name*
18. **exit**
19. **interface** *type number*
20. **zone-member security** *zone-name1*
21. **exit**
22. **interface** *type number*
23. **zone-member security** *zone-name*
24. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map type inspect match-any** *class-map-name* **Example:**	Creates an inspect type class map and enters class-map configuration mode.

	Command or Action	Purpose
	`Router(config)# class-map type inspect match-any rtsp_class1`	
Step 4	**match protocol** *protocol-name* **Example:** `Router(config-cmap)# match protocol rtsp`	Configures the match criteria for a class map on the basis of the named protocol. • Use DNS in place of RTSP to configure DNS as the match protocol.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	Returns to global configuration mode.
Step 6	**policy-map type inspect** *policy-map-name* **Example:** `Router(config)# policy-map type inspect rtsp_policy`	Creates an inspect type policy map and enters policy-map configuration mode.
Step 7	**class type inspect** *class-map-name* **Example:** `Router(config-pmap)# class type inspect rtsp_class1`	Specifies the class on which the action is performed and enters policy-map-class configuration mode.
Step 8	**inspect** **Example:** `Router(config-pmap-c)# inspect`	Enables stateful packet inspection.
Step 9	**class class-default** **Example:** `Router(config-pmap-c)# class class-default`	Specifies that these policy map settings apply to the predefined default class. If traffic does not match any of the match criteria in the configured class maps, it is directed to the predefined default class.
Step 10	**exit** **Example:** `Router(config-pmap-c)# exit`	Returns to policy-map configuration mode.
Step 11	**exit** **Example:** `Router(config-pmap)# exit`	Returns to global configuration mode.
Step 12	**zone security** *zone-name1* **Example:**	Creates a security zone to which interfaces can be assigned and enters security-zone configuration mode.

	Command or Action	Purpose
	`Router(config)# zone security private`	
Step 13	**exit** **Example:** `Router(config-sec-zone)# exit`	Returns to global configuration mode.
Step 14	**zone security** *zone-name2* **Example:** `Router(config)# zone security public`	Creates a security zone to which interfaces can be assigned and enters security-zone configuration mode.
Step 15	**exit** **Example:** `Router(config-sec-zone)# exit`	Returns to global configuration mode.
Step 16	**zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name* **Example:** `Router(config)# zone-pair security pair-two source private destination public`	Creates a pair of security zones and enters security-zone-pair configuration mode. • To apply a policy, you must configure a zone pair.
Step 17	**service-policy type inspect** *policy-map-name* **Example:** `Router(config-sec-zone-pair)# service-policy rtsp_policy`	Attaches a firewall policy map to the destination zone pair. • If a policy is not configured between a pair of zones, traffic is dropped by default.
Step 18	**exit** **Example:** `Router(config-sec-zone-pair)# exit`	Returns to global configuration mode.
Step 19	**interface** *type number* **Example:** `Router(config)# GigabitEthernet0/1/0`	Specifies an interface for configuration. • Enters interface configuration mode.
Step 20	**zone-member security** *zone-name1* **Example:** `Router(config-if)# zone-member security private`	Assigns an interface to a specified security zone. • When you make an interface a member of a security zone, all traffic into and out of that interface (except traffic bound for the router or initiated by the router) is dropped by default. To let traffic through the interface, you must make the zone part of a zone pair to which you apply a policy. If the policy permits traffic, traffic can flow through that interface.

	Command or Action	Purpose
Step 21	**exit** **Example:** `Router(config-if)# exit`	Returns to global configuration mode.
Step 22	**interface** *type number* **Example:** `Router(config)# GigabitEthernet0/1/0`	Specifies an interface for configuration. • Enters interface configuration mode.
Step 23	**zone-member security** *zone-name* **Example:** `Router(config-if)# zone-member security public`	Assigns an interface to a specified security zone. • When you make an interface a member of a security zone, all traffic into and out of that interface (except traffic bound for the router or initiated by the router) is dropped by default. To let traffic through the interface, you must make the zone part of a zone pair to which you apply a policy. If the policy permits traffic, traffic can flow through that interface.
Step 24	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Troubleshooting Tips

The following commands can be used to troubleshoot your RTSP-enabled configuration:

- **clear zone-pair**
- **show policy-map type inspect zone-pair**
- **show zone-pair security**

Configuration Examples for vTCP for ALG Support

Example RTSP Configuration

The following example shows how to configure the RTSP inspection:

```
class-map type inspect match-any rtsp_class1
match protocol rtsp
policy-map type inspect rtsp_policy
class type inspect rtsp_class1
inspect
class class-default
zone security private
```

```
zone security public
zone-pair security pair-two source private destination public
service-policy type inspect rtsp_policy
interface GigabitEthernet0/1/0
 ip address 10.0.0.1 255.0.0.0
zone-member security private
!
interface GigabitEthernet0/1/1
 ip address 10.0.1.1 255.0.0.0
  zone-member security public
```

Additional References for vTCP for ALG Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS firewall commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z
Cisco Firewall--SIP Enhancements: ALG	*Security Configuration Guide: Securing the Data Plane*
Network Address Translation	*IP Addressing Services Configuration*

Standards and RFCs

Standard/RFC	Title
RFC 793	*Transport Control Protocol*
RFC 813	*Window and Acknowledge Strategy in TCP*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html